BNFL Inc.

Section 3.0

Category 2 Introduction

Contents

Item | Page Number

Section 3.0 Category 2 Introduction

FIGURES

Contents

Section 3.0
Category 2 Introduction

3.0.1. Example Descriptions

This section presents ten representative examples of the application of the integrated safety management process to systematically define important-to-safety (ITS) structures, systems and components (SSCs) and their design safety features (DSFs). They demonstrate how BNFL Inc. design strategies and equipment performance criteria will provide protection for workers, and the public. This introduction includes general information that is applicable to all ten examples.

The ten examples were proposed by BNFL Inc., with concurrence by the DOE RU. They were selected to give a range of unmitigated consequences and hazard types as requested by DOE. The BNFL Inc. design will incorporate defense in depth through prevention and mitigation features that include robust ITS SSCs with appropriate DSFs to ensure protection of the facility worker, the co-located worker and the public. The examples were chosen based on assessments in the Hazard Analysis Report (HAR), judgment and experience. The ten examples are:

1. **Hydrogen Generation in the High Level Waste Storage Vessels**. This event involves the generation of hydrogen in High Level Waste storage vessels due to radiolysis of water. It was selected because it could lead to an explosion that would result in high consequences for facility and co-located workers and moderate consequences for the public. Also, the subject of explosive hazards is an open issue from Part A. This example evaluates the issue with respect to the hydrogen explosive hazard in the High Level Waste storage vessels. The resulting strategy potentially has broad application to various other vessels.

2. **Loss of Cooling to the Cesium Storage Vessel**. This event involves the potential hazards associated with boiling of the cesium storage vessel contents due to the decay heat generated by the high activity of the concentrated cesium. It was selected because it was judged to be of low consequence for workers and the public.

3. **Load Drop of a Pretreatment Pump (Out of Cell)**. This event involves dropping a cask (flask) containing a contaminated High Level Waste pretreatment pump during transport from its cell to a maintenance facility. It was selected to provide an example of a hazard that has potential to primarily affect the facility worker. It was judged to be a high consequence event for the facility worker and low consequence for the co-located worker and the public.

4. **High Level Waste Melter Feed Line Failure**. This event involves a breach of the High Level Waste melter feed line and release of process material into the cell. It was selected because it is an example of a spill of high level waste and was judged to be a high consequence event for workers and moderate consequence for the public.

5. **Cooling Water Contamination**. This event involves a failure of the cooling coil in the High Level Waste blending vessel. It was selected to provide an example of a direct radiation exposure event. It was judged to be a low consequence event for the workers and the public.

6. **Sample Carrier Breakout**. This event involves breakout of a sample carrier from the pneumatic sample transfer system. It was selected to provide an example of a hazard that has potential to primarily affect the facility worker. It was judged to be a high consequence event for the facility worker and low consequence for the co-located worker and public.

7. **Low Activity Waste Pipe Break**. This event involves a break in the Low Activity Waste transfer pipe between the tank farm and the pretreatment facility. It was selected because it provides an example of an event external to the facility. It was judged to be a moderate consequence event for the facility and co-located workers and low consequence for the public.

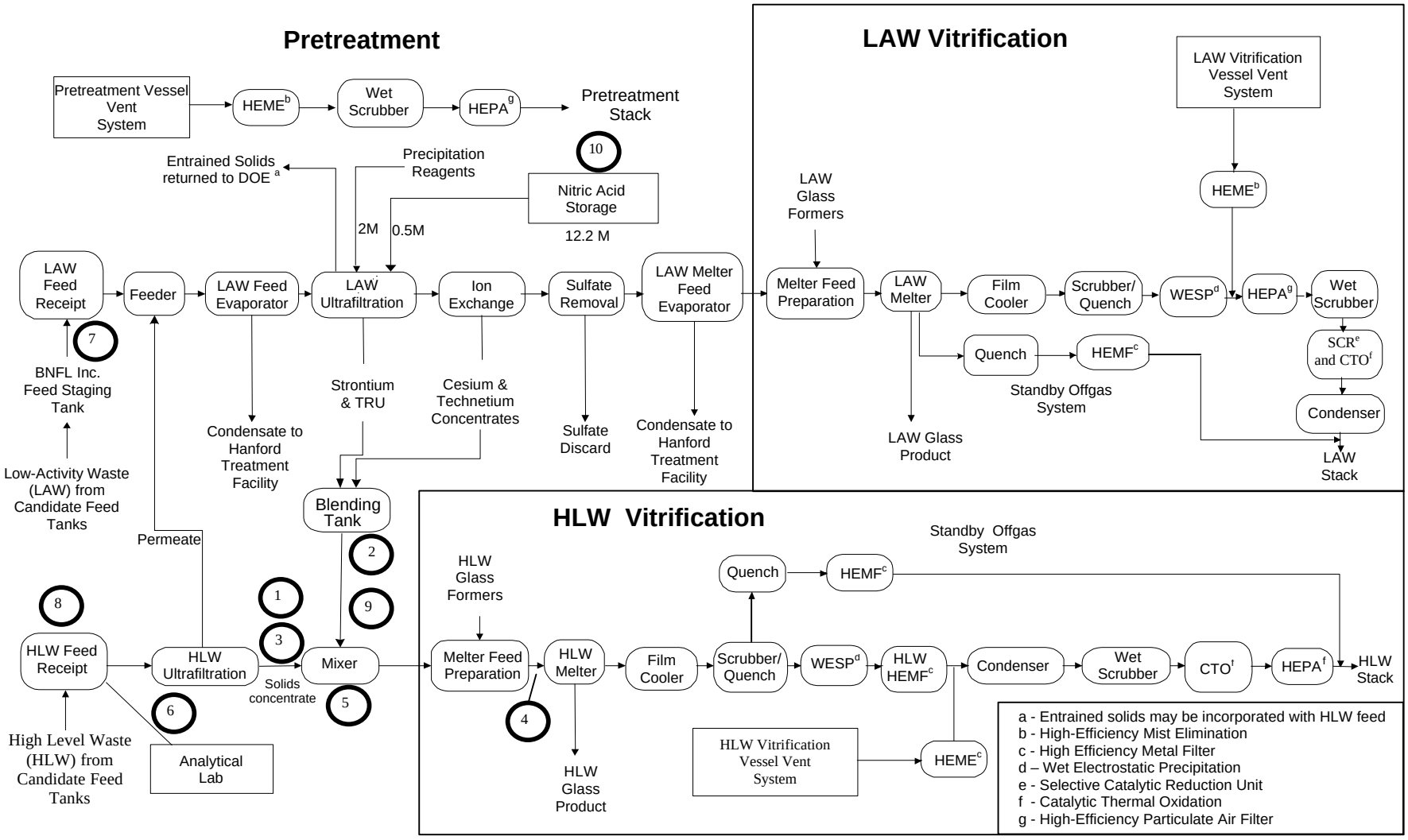
8. **Receipt Vessel Rupture**. This event involves the rupture of the High Level Waste receipt vessel in the pretreatment area. It was selected because it was judged to be a high consequence event for the workers and the public.

9. **Activity Backflow From a Process Vessel Into the Vessel Wash Cabinet**. This event involves the potential for backflow of radioactive material up the wash line into the wash cabinet in the operations area. It was selected because it has the potential for external and/or internal radiation exposure. It was judged to be a moderate consequence event for the facility worker and low consequence for the co-located worker and public.

10. **Nitric Acid Handling**. This event involves a nitric acid spill at the unloading facility. It was selected because it provides an example that deals with process safety as opposed to radiological safety. It was selected because it was judged to be a high consequence event for the facility worker, moderate consequence for the co-located worker and low consequence for the public.

These ten events represent potential hazards at various locations in the process. Figure 3.0-1 shows where each of the events appears in the process flow diagram. Also, it should be noted that these examples are in an early stage of detail design, so design assumptions were required for completion of these analyses. Some examples required more assumptions than others do. It should also be noted that the expected consequences for the ten examples were based on evaluations in the Part A HAR (BNFL Inc 1998a) and ISAR (BNFL Inc 1998b). The evaluated consequences in the ten examples do not always match the expectations because of evolution in scenario development and analysis since Part A.

Figure 3.0-1. Location of Examples in Process..



Some of these examples were previously evaluated as hazards and documented in the HAR and ISAR. For these examples, this analysis builds on this previous work. Others were not specifically identified previously and for these examples this constitutes an initial analysis. Table 3.0-1 identifies where example topics (or related topics) were previously documented, and what additional information is provided by this deliverable.

Table 3.0-1. Status of Examples in Previous Hazard Analysis.

EXAMPLE TOPIC	HAR	ISAR	COMMENT
1. Hydrogen Generation in the High level Waste Storage Vessels	Page 5-57, Event 1614666/122. Generic (No specific tanks or protective strategy)	Page 4-141, Table 4-31, event 30. Different tank, same type hazard.	Presented at the January 1999 topical meeting. Example involves a greater consequence and more detailed control strategy.
2. Loss of Cooling to the Cesium Storage Vessel	Page 5-102, event 1614667/153.	Page 4-136, Table 4-30, event 8.	Example carries previous analysis to more detail.
3. Load Drop of a Pretreatment Pump (Out of Cell)	Not included	Not included	Example represents initial hazard analysis.
4. High Level Waste Melter Feed Line Failure	Page 5-131, Event 3200/160.	Page 4-133, Table 4-29, event 6.	Hazard was identified but not analyzed. Example represents initial hazard analysis.
5. Cooling Water Contamination	Page 5-80, Event 1614662/131.	Not included	Hazard was identified but not analyzed. Example represents initial hazard analysis.
6. Sample Carrier Breakout	Not included	Not included	Example represents initial hazard analysis.
7. Low Activity Waste Pipe Break	Page 5-15, event 0/47, erosion/corrosion. Page 5-16, event 0/51, rupture due to mechanical digging activities. Page 5-16, event 0/39, water hammer. Page 5-17, event 0/49, extreme weather.	Page 4-130, event 1, Seismic Damage To Transfer Line.	ISAR references analyses of waste pools in the TWRS BIO. Surface pool formed and resulting exposures are expected to be much less at TWRS-P than those postulated in the TWRS Basis for Interim Operation bounding analysis. Example carries previous analysis to more detail.
8. Receipt Vessel Rupture	Page 5-151, event 3200/220. Different tank from ISAR.	Page 4-153, Section 4.7.2.2. Also on Page 4-180, in Table 4-45, Section 4.7.2.2.	Example carries previous HAR analysis to more detail.
9. Activity Backflow from a Process Vessel into the Vessel Wash Cabinet	Page 5-98, event 1614667/1, pressurization for nitric acid recovery, and page 5-257, event 1614683/125, siphoning, diffusion and backflow for outcell process reagents.	Not included	Previous analyses looked at cross contamination due to backflow into outcell reagent lines. This example looks at hazards due to backflow into wash lines.

Table 3.0-1. Status of Examples in Previous Hazard Analysis.

EXAMPLE TOPIC	HAR	ISAR	COMMENT
10. Nitric Acid Handling	Page 5-101, Event 1614667/117 addresses a spill in the process building.	Page 4-171, Section 4.7.2.9. Also on Page 4-179 in Table 4-44. A 5,000 gal tank – 12.2M acid spill in wet chemical storage area.	A separate hazard analysis (BNFL Inc.-5193-RTP-006, Rev. 0, Preliminary Safety Review of TWRS-P Bulk Cold Chemical Storage Systems) addressed nitric acid. Example expands one aspect of the previous analysis in the ISAR.

The ten events were not purposely selected to identify the design basis event(s) (DBE) that would establish the bounding performance requirements of the mitigative or preventive ITS SSCs. The events were selected, among other reasons, to give a range of consequences. For those events that have an SSC whose only safety function is to prevent or mitigate the event analyzed, it is likely that DBE for that SSC has been identified. For other events, such as the Receipt Vessel Rupture that credits mitigation by the C5 extract system, additional safety analysis will need to be performed before it can be concluded that the DBE for this system has been identified.

Uncertainties in the design and accident consequence analysis that, upon resolution, may result in challenging the radiological exposures standards, have been accommodated by selecting preferred control strategies (including SSCs and DSFs) that result in estimated exposures to the facility workers, co-located workers, and the public that are significantly below the radiological exposure standards. This is apparent by review of the Section 3.x.5.3, “Mitigated Consequences” for the radiological examples presented.

The margin of safety has been enhanced by the preference for prevention over mitigation, and passive over active features. For example, prevention has been selected for the following cases:

1. Hydrogen Generation in the High Level Waste Storage Vessels (maintain the hydrogen concentration below the lower flammability limit)

2. Loss of Cooling to the Cesium Storage Vessel (vessel size to facilitate natural convection cooling)

3. Cooling Water Contamination (detect small coil leaks prior to tube break; the radiological consequences of a small leak are estimated)

4. Low Activity Waste Pipe Break (prevent excavation access to the transfer line)

5. Activity Backflow From a Process Vessel into the vessel wash cabinet (barometric head protection by piping layout).

In the evaluation of radiological events, no credit was taken for immediate operator action.

The consequence and frequency analyses in the ten examples are bounding for the following reasons.

1. The material at risk in each example is based on the maximum mass of material that could be affected in the scenario and on the most consequential isotopic composition that could be present.

2. The respirable release fractions in the analyses are the maximum values appropriate for the release scenario under consideration.

3. Leak path factors in the analysis are also appropriate for the release scenario under consideration.

4. The respirable release fractions and leak path factors in the analysis are from BNFL or DOE sources and are based on conservative evaluations of experimental data.

5. Decontamination factors used in the analyses are consistent with accepted nuclear industry practice for accident analyses.

6. The atmospheric dispersion factors in the analyses are consistent with the requirements of USNRC Regulatory Guide 1.145.

7. The frequency assessments are conservatively structured so that the results represent upper bound estimates of the frequency of the event under consideration.

3.0.2. Identification of Structures, Systems and Components

3.0.2.1. Implementing Procedures

BNFL Inc. uses procedure K71P505, *Safety Standards and Requirements Identification* (BNFL Inc. 1998c), to implement the process mandated by DOE/RL-96-0004. Procedure K71P505 references the set of procedures, codes of practice, and design guides employed by BNFL Inc. at each step of the DOE/RL-96-0004 process.

3.0.2.2. Process Steps

The three DOE documents that form the basis of this deliverable are 98-RU-0329 which describes the integrated safety management process elements to be incorporated, DOE/RL-0004 (DOE-RL 1998a) which describes the process, and DOE/RL-0006 (DOE-RL 1998b) which contains top level standards and principles. These example events were analyzed using the process steps described in BNFL Inc. procedure K71P505 for safety standards and requirements identification (BNFL Inc. 1998c). This procedure is a flowdown of the essential process steps mandated by DOE/RL-96-0004. Table 3.0-2 shows how the procedure steps relate to the mandated steps, the integrated safety management process elements (from 98-RU-0329) and to top-level principles, and where they are documented in this deliverable.

Table 3.0-2. Process Steps and Where Documented.

DOE/RL-96-0004	BNFL Inc. K71P505	DSF Scope and Content (98-RU-0329)	BNFL Inc. DSF Deliverable
1. Process Initiation	1. Initiate Process	Not Specifically Addressed	3.0 Category 2 Introduction
2. Identification of Work	2. Identify Work	Not Specifically Addressed	3.X.1 Work Identification
3. Hazards Evaluation	3. Hazards Evaluation	1. Identification of hazards and the methodology used for identification of hazards. 4. DBE descriptions and justifications that these envelope known safety concerns.	3.X.2 Hazard Evaluation 3.X.2 Hazard Evaluation
4. Development of Control Strategies	4. Development of Control Strategies	2. Identification of Hazard Control Strategies and the overall approach used to select/define these Control Strategies. 5. SSCs relied on to assure that consequences to the worker and the public from DBEs meet the top-level Safety Standards and Principles (DOE/RL-96-0006) with adequate certainty and margin (i.e. SSCs relied on for safety).	3.X.3 Control Strategy Development 3.X.5 Control Strategy Assessment 3.X.3 Control Strategy Development 3.X.6 Conclusions and Open Issues
5. Identification of Standards	5. Identification of Standards	2. Design safety features required to implement Hazard Control Strategies. 6. Measures (including design standards and administrative measures) to assure availability and reliability of SSCs relied on for safety.	3.X.4 Safety Standards and Requirements 3.X.4 Safety Standards and Requirements
		7. Process for identifying and justifying measures.	3.X.4 Safety Standards and Requirements
6. Confirmation of Standards	6. Confirmation of Standards	Not Specifically Addressed	DSF Submittal approved by the PSC
7. Formal Documentation	7. Formal Documentation	Not Specifically Addressed	DSF Submittal
8. Recommendation by Contractor Representative	7. Formal Documentation	Not Specifically Addressed	DSF Submittal

This process establishes an orderly procedure to prepare these Category 2 examples. The first process step involves allocating and organizing adequate resources to perform the task. BNFL Inc. assembled a Category 2 Team to implement the integrated safety management process. Operating guidelines were prepared, deliverables were identified, and deadlines established. Daily team meetings were held to discuss guidance, schedule and other issues common to all ten examples.

Members of the Category 2 Team were then assigned as “core teams” for the ten examples in groups of four to seven individuals with appropriate technical backgrounds. Each “core team” performed the

combined functions of the "Multi-discipline Design Team" and the "Safety Standards and Requirements Team/Hazard Analysis Team" described in BNFL Inc. procedure K71P505. Table 3.0-3 lists the core team members with their titles and roles on the teams. As shown in the table, many individuals were members of more than one team.

The core teams were responsible for implementing the integrated safety management process for their particular example and documenting their results for this deliverable. They prepared and presented storyboard peer reviews and held team meetings to analyze the hazards and develop control strategies. They used K71P505 and other applicable project procedures and implementing standards as required. Each team was assigned a team leader who was responsible for providing coordination and leadership. Other TWRS-P organizations provided support as required.

Table 3.0-3. Core Team Members Assigned to Examples.

NAME	TITLE	ROLE	**Example** [See Table 3.0-1 for example titles]									
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Allen, Todd	Safety Engineer	Writer.		X		X	X					
Anderson, Ted	Senior Process Engineer	Checker/Reviewer		X								
Boomer, Kayle	Technical Manager-Waste Chemistry	Provided process details and source terms.	X	X	X	X	X	X	X	X	X	
Bostock, Steve	Project Operations Coordinator	Provided operations input.	X	X	X	X	X	X	X	X	X	X
Carro, Craig	Safety Engineer	Team Lead for 7.							X			
Cullen, Bob	Safety Manager	Team Lead for 9. Writer.									X	
Curry, Lynn	Hazard & Safety Analysis Lead (High Level Waste)	Team Lead for 2, 4, & 5.		X		X	X					
Davies, Brian	Design Manager -Pretreatment	Provided engineering details.	X								X	
Eaton, Will	Melter Liaison Engineer (High Level Waste)	Provided technical design and process information.				X						
Garrett, Dave	Senior Safety Assessor	Writer. Provided overall technical direction.			X							
Hinckley, John	Hazard &Safety Analysis Lead (Low Activity Waste)	Writer.	X							X		
House, Bill	Procedure Preparation Engineer	Writer					X					
Johnson, Scott	Safety Engineer	Writer										X
Kempsell, Ian	Deputy Safety & Regulatory Program Manager	UK expert on hydrogen.	X									
Kloster, Gary	Mechanical Engineering Specialist	Provided detailed fluid system information.										X
Kolaczkowski, Alan	Reliability Engineer	Provided frequency/reliability analysis.	X	X	X	X	X	X	X	X	X	X
Kummerer, Maryanne	Safety Engineer	Consequence analysis.	X						X	X		
Larson, Andy	Design Safety Implementation Deputy Manager	Team Lead for 1.	X									

Table 3.0-3. Core Team Members Assigned to Examples.

NAME	TITLE	ROLE	Example [See Table 3.0-1 for example titles]									
			1	2	3	4	5	6	7	8	9	10
Larson, Don	Senior Engineer High Level Waste Vitrification	Provided engineering input and analyses.				X						
Lindquist, Chris	Safety Engineer	Analysis	X									
Magraw, Rob	Safety Engineer	Team Lead for 6. UK expert on sampling.						X				
McDonnell, Tom	Safety Engineer	Writer	X									
Moomey, Harry	Hazard &Safety Analysis Lead (BOF)	Team Lead for 3. Safety advisor.			X							X
Mottram, Joanne	Safety Engineer	Team Lead for 8. Writer.								X		
Naretto, Chuck	Safety Engineer	Writer. Provided safety engineering input.			X							X
Papp, Ivan	Process Engineering Lead	Provided detailed process information.							X			
Reddick, Julie	Process Engineer	Writer.						X				
Richardson, John	Mechanical Engineering Lead	Provided detailed mechanical information.			X			X				
Roth, Janet	Process Engineer	Team Lead for 10.					X					X
Skeath, David	Piping Engineer	Provided engineering support.							X			
Smith, Dean	Safety Engineer	Consequence analysis			X	X	X	X				
Sontag, Steve	Safety Engineer	Consequence analysis and report writing.		X		X	X					
Steele, Dave	Lead Mechanical Engineer	Writer. Provided engineering input.			X							
Thomson, Scott	Process Engineer	Provided detailed process information.				X		X				
Vickers, Dave	Process Lead	Provided technical design and process information.					X					
Wojdac, Larry	Safety Engineer	Provided safety analysis/technical input.		X								X
Wright, Steve	Principle Lead Engineer	Provided engineering input/analysis.									X	

3.0.2.3. Hazard Analyses

3.0.2.3.1. Analysis of Radiological Events

BNFL Inc uses consequence severity levels (SLs) and event target frequencies to guide development of control strategies for radiological events. To determine the severity level for a radiological consequence, the unmitigated consequences are first evaluated without consideration for SSCs that serve to prevent or mitigate the release. Credit is taken for passive features such as the cell walls and back diffusion filters if they are not challenged by the event. SLs are determined for the worker, co-located worker and the public at the locations specified in Attachment F to the SRD, Volume I (BNFL Inc. 1998d). The radiological SLs as defined in Attachment A to the SRD, Volume II (BNFL Inc. 1998e) are listed in Table 3.0-4. SLs range from SL-1 for the highest (most severe) consequence to SL-4 for the lowest (least

severe). The frequency of occurrence for the initiating event is also estimated. Environmental impacts will be assessed as part of the Environmental Report submitted to support the Operating License Request.

Table 3.0-4. Radiological Severity Levels.

SL	Facility Worker Consequence	Co-Located Worker Consequence	Public Consequence
SL-1	>25 rem/event	>25 rem/event	>5 rem/event
SL-2	5 – 25 rem/event	5 – 25 rem/event	1 – 5 rem/event
SL-3	1 – 5 rem/event	1 – 5 rem/event	0.1 – 1 rem/event
SL-4	<1 rem/event	<1 rem/event	<0.1 rem/event

Next, the highest consequence SL for the event is used to determine the target frequency from Table 3.0-5 which is reproduced from Appendix A of the SRD Volume II (BNFL Inc. 1998e). This table defines the target frequency for a given severity level. As expected, the higher the consequence SL the lower the corresponding event target frequency. The target frequency is the frequency of occurrence to be obtained with the selected control strategy in effect. The target frequency divided by the frequency of occurrence for the initiating event gives the target reliability requirement for the control strategy.

Table 3.0-5. Target Frequencies.

SL	Event Target Frequency (y^{-1})
SL-1	$<10^{-6}$
SL-2	$<10^{-4}$
SL-3	$<10^{-2}$
SL-4	$<10^{-1}$

When necessary, assurance that the target frequency is likely to be met by the selected control strategy is accomplished by constructing reliability models for the accident initiator and the corresponding selected control features. These models consist of fault trees of the postulated control strategy equipment and associated human actions planned to prevent or mitigate exposure to the hazard(s) of concern. The fault-tree based reliability models for these examples are computerized using a validated computer code developed for such purposes and which has been used extensively in nuclear power plant probabilistic risk assessments for almost two decades. It is called the CAFTA® code, a software product of one of the BNFL Inc team members with Electric Power Research Institute sponsorship. The code has been used on projects requiring quality assurance commensurate with 10CFR Part 50, Appendix B or NQA-1 requirements.

Reliability data needed to obtain the quantitative result come from five sources supplemented with additional conservative judgment where needed. These sources were chosen because they represent both relevant experience at BNFL's Sellafield site (Sellafield 1998) with activities quite similar to those planned for TWRS-P, as well as reliability experience data from nuclear, chemical, and industrial sources combined into a “generic” database used at Savannah River (Blanton 1993). Two sources (Atwood 1998 and Marshall 1998) represent the latest work useful to reliability studies requiring the estimation of losses of power and common cause failure potential, both under the sponsorship of the US Nuclear Regulatory

Commission. The fifth source (Swain 1983) is a well-recognized and often used source for human reliability estimation by human reliability analysts working on both DOE and NRC nuclear application programs.

3.0.2.3.2. Analysis of Hazardous Chemical Events

In accordance with Safety Criterion 2.0-2 in volume II of the SRD (BNFL Inc. 1998e), when the consequences of a potential chemical release is projected to be above the Emergency Response Planning Guide-2 (ERPG-2), it is required that the hazard be evaluated and measures be taken to prevent the accident or mitigate the consequences of an accident. When an ERPG-2 limit has not been published for a chemical (e.g., nitric acid), the Temporary Emergency Exposure Limits (TEEL) are used. The term TEEL describing interim, temporary, or equivalent exposure limits for which official ERPGs have not yet been developed, was adopted by the Department of Energy (DOE) Subcommittee on Consequence Assessment and Protective Actions at its April 1996 meeting in Knoxville, Tennessee. The process hazard evaluation may be performed using one of several acceptable industry practices such as a "what if" process, a formal checklist, HAZOPS, etc., as prescribed in 29CFR1910.119, Process Safety Management of Highly Hazardous Chemicals.

Where the hazards are similar to commercial industry hazards, (e.g., Nitric Acid Handling example), it is acceptable to adopt industry standards, then examine if additional control strategies would add significant safety benefit. Where such strategies have been identified, they are adopted as long as they do not have significant effects on operability, etc. These evaluations are performed deterministically. The results of the evaluation should ensure that the design and administrative measures incorporate good practices and lessons learned from the commercial industry. For bulk storage of chemicals used at TWRS-P, the techniques and candidate strategies for handling such chemicals have been well developed by the chemical industry and are well accepted.

Section 4.3.1 in Appendix A, Volume II of SRD (BNFL Inc. 1998e) states that when the ERPG-2 limits are postulated to be exceeded, the full extent of the Process Safety Management (PSM) program should be applied. The design elements are examined to ensure that their incorporation will facilitate the implementation of a PSM program.

3.0.2.4. Designation of Structures, Systems and Components

The elements comprising a hazard control strategy shall have standards and requirements applied that affect their design, construction, operation, maintenance, or testing. To ensure that these requirements are properly addressed, all SSCs having safety functions essential to meet the guidelines in the Safety Requirements Document Vol. I, Appendix F (SRD) are designated "Important to Safety" (ITS). Therefore, the SSCs that are essential to ensuring the safety functions associated with the hazard control strategy are designated as being Important to Safety. This designation alerts personnel who are working with such an SSC (i.e., designing, constructing, operating, etc.) that the SSC has a safety function, and that special standards and requirements may exist. Changes to SSCs designated as Important to Safety are subject to configuration management to ensure that the required safety function is maintained.

3.0.2.5. Approach to Implementation of Defense In Depth

BNFL Inc.'s defense in depth implementing procedure flows from DOE's top level principles (DOE/RL-96-0006). Defense in depth is a safety design concept or strategy that is applied at the beginning of design activities and maintained throughout the facility life. This safety design strategy is

based on the premise that no one level of protection is completely relied on to ensure safe operation. Defense in depth is the provision of multiple layers of protection appropriate to the hazard severity to prevent or mitigate an unintended release of radioactive or hazardous chemical material to workers, or the public. Defense in depth is established in the "Implementing Standard for Defense in Depth", which is part of the *Safety Requirements Document* (BNFL Inc. 1998b), and is implemented via BNFL Inc. Code of Practice K70C514 (BNFL Inc 1998c).

3.0.3. Identification of Design Safety Features

DSFs are derived based on the existing BNFL Inc. process for identifying the critical design and administrative features associated with an SSC. They consist of the important attributes that enable and ensure the ITS SSC can perform its safety function with appropriate reliability and operational availability and meet or exceed the necessary consequence/frequency combination to operate the facility in accordance with environmental, safety and health standards, defense in depth protection and ALARA.

Usually a DSF will be an attribute of a specific SSC, with the exception of generic DSFs. The facility will include a group of generic DSFs that apply to all ITS SSCs as described in the Category I Introduction (Section 2.0 of this deliverable).

3.0.4. Identification of Standards

3.0.4.1. Process for Standards Identification

Identification of standards is an iterative process. An initial set of standards and requirements is derived from a preliminary determination of the hazards and potentially hazardous situations inherent in the work. As the design evolves, an improved hazard evaluation and further development of the control strategies justify tailoring the set of standards. The aim of this activity is to identify an appropriate set of standards and requirements that will assure adequate safety when implemented.

Based on the set of evaluations and analyses performed in Part A, BNFL Inc. conservatively identified applicable codes and standards in the SRD. BNFL Inc. Basis of Design document, while compliant with its SRD commitments, identified additional standards, including commercial standards, applicable to the overall facility design.

For the category 2 examples, a group of standards, including those committed in the SRD, were identified for consideration. Where the analysis established performance requirements for an ITS SSC, the SRD codes and standards were considered by experienced personnel along with other standards that may be appropriate for the specific event under evaluation. The standards complementing a robust design are expected to be sufficient to support the performance requirements of the specific control strategy for the hazard evaluated.

It should be noted that codes and standards applicable for one specific hazard and reliability target may not, when analyses are completed, be the determining ones, as systems have to be evaluated for the totality of their design requirements. Also, they may not conform one-for-one with the full set of standards in the SRD. These initial selections will receive scrutiny for potential revision several times as the design matures. The project processes for maintaining compliance with the Authorization Basis will assure conformance with the standards identified in the SRD as the design develops.

3.0.4.2. Measures to Assure Availability, Maintainability and Reliability of SSCs

Reliability targets are assigned to ITS SSCs together with a program requiring periodic testing and inspection of these components. Previous experience at other BNFL facilities and proven design and engineering practices with SSCs are used in assuring availability, maintainability, and inspectability of the SSCs. A testing program identifies proper functioning, correct design, and the detection and correction of any design errors.

3.0.5. Format of Category 2 Information

The information for each of the ten representative examples is presented in six subsections. The "X" in the section number varies from 1 to 10 and identifies the specific example in sequence. The subsections and a summary of their content are as follows:

Work Identification (3.X.1)

This subsection develops a general description of the work for use in the hazard evaluation in the next subsection, based on current design documentation. It includes key process and design parameters, interfaces, operating environment, and applicable experience

Hazard Evaluation (3.X.2)

This subsection identifies and evaluates, a hazard and an initiator. Severity level, ERPG or TEEL limit, frequency of occurrence and target frequency are determined. Natural phenomena hazards (NPHs), man-made external events, and common cause events that may have an impact are identified. In the normal process, all initiators related to an example event would be analyzed and a corresponding control strategy developed; however, to demonstrate application of the entire process for this deliverable, one event sequence was selected for each example. The rationale used to select each of the hazards is presented.

Control Strategy Development (3.X.3)

This subsection identifies potential control strategies based on proven BNFL and industry engineering practices. These strategies are then evaluated for control effectiveness, practicality, demonstrability, reliability, compliance with laws and regulations, and ability to comply with the top-level principles in DOE/RL-96-0006. The strategies selected for further consideration are then evaluated for: introduction of secondary hazards, impact on other safety features, impacts of other hazards on the control strategy, robustness to other fault conditions (including seismic and other NPHs), passive or active, robustness of any administrative controls required, cost, operability, maintainability, and ease of justification. The final control strategy is selected with the objective of meeting the target frequency for the event. Then, ITS SSCs that implement the control strategy are described. Some DSFs that support the ITS SSCs may be included in this section.

Safety Standards and Requirements (3.X.4)

This subsection describes the design safety features, administrative measures, design standards, reliability targets, performance requirements, and any other requirements for the SSCs identified in the previous subsection. Any standards not currently in the SRD (BNFL Inc. 1998e) are noted.

Control Strategy Assessment (3.X.5)

The selected control strategy in each of the ten examples has been evaluated against a set of relevant top-level radiological, nuclear and process safety standards and principles in DOE/RL-96-0006 (DOE-RL 1998b). The detailed discussions in each of the ten example reports demonstrate BNFL's compliance with those top-level principles that are relevant to the control strategies.

This subsection also addresses the following topics in accordance with the BNFL Inc. Implementing Standard for Safety Standards and Requirements Identification (BNFL Inc. 1998c) procedure and associated code of practice (BNFL Inc. 1998f):

- Mitigated consequence evaluation: summarizes the calculation that evaluates the consequences of the release for the example, given that all mitigation systems function as designed.

- Frequency of the mitigated event (initiating event plus failure of the preventive mechanisms): provides an evaluation of the frequency with which radioactivity could be released. This frequency evaluation includes consideration of common mode failures. It also considers common cause failures such as loss of power.

- Consequence evaluation assuming complete failure the control strategy: summarizes the calculation that evaluates the consequences of the release for the example, given that all mitigation systems fail. This evaluation considers all inherent passive barriers that are not challenged by the scenario remain intact. For example, in cell retention, building wake, etc.

- Frequency of the control strategy failure (initiating event plus failure of all prevention and mitigation mechanisms): summarizes the frequency of the release associated with the initial event scenario and may include a discussion of methods to lower the frequency or lessen the severity level of the event, even with failed mitigation strategies.

Conclusions and Open Issues (3.X.6)

This subsection presents the conclusions drawn from each example and summarizes the assumptions and open issues that were identified. Subsequent to completion of this deliverable, the assumptions and open issues identified in these examples will be retained as open issues in the Safety and Regulatory Programs (S&RP) Tracking System to be completed at the appropriate stage of design development.

3.0.6. Definitions

Certain terms will be encountered throughout these examples that are important to the conclusions presented. They will be in bold text as a tool to aid subsequent collation and have the following meanings:

- **Design Assumption**: An aspect of the design that was used in determining consequence or frequency for use in these examples. Change of this parameter could affect the validity of the safety argument.

- **Operational Assumption**: An aspect of facility operation that was used in determining consequence or frequency for use in these examples. Change of this parameter could affect the validity of the safety argument.

- **Open Issue**: Unresolved issue that has been identified as needing to be defined to resolve a design or operational question.

- **Safety Function**: Any function that is necessary to ensure: 1) the integrity of the boundaries retaining the radioactive materials, 2) the capability to place and maintain the facility in a safe state, or 3) the capability to prevent or mitigate the consequences of facility conditions that could result in radiological exposures to the general public or workers in excess of appropriate limits. (DOE-RL 1998b)

References

Atwood C. et al., 1998, "Evaluation of Loss of Offsite Power Events at Nuclear Power Plants: 1980-1996," NUREG/CR-5496, Idaho National Engineering and Environmental Laboratory for the U.S. Nuclear Regulatory Commission, November 1998.

Blanton, 1993, C. Blanton and S. Eide, "Savannah River Site Generic Data Base Development," WSRC-TR-93-262, Westinghouse Savannah River Company, June 30, 1993.

BNFL Inc., 1998a, *Hazard Analysis Report*, BNFL-5193-HAR-01, Rev. 0, BNFL Inc., Richland, Washington.

BNFL Inc., 1998b, *Initial Safety Analysis Report*, BNFL-5193-ISAR-01, Rev. 0, BNFL Inc., Richland, Washington.

BNFL Inc., 1998c, *Safety Standards and Requirements Identification*, K71P505, Rev. 0, BNFL Inc., Richland, Washington, November 1998.

BNFL Inc., 1998d, *Safety Requirements Document, Volume I*, BNFL-5193-SRD-01, Rev. 2, BNFL Inc., Richland, Washington, December 1998.

BNFL Inc., 1998e, *Safety Requirements Document, Volume II*, BNFL-5193-SRD-01, Rev. 2, BNFL Inc., Richland, Washington, December 1998.

BNFL Inc., 1998f, *Code of Practice for Development of Hazard Control Strategies and Identification of Standards*, K70C514, Rev. 0, BNFL Inc., Richland, Washington, November 1998.

DOE-RL, 1998a, *Process for Establishing a Set of Radiological, Nuclear, and Process Safety Standards and Requirements for TWRS Privatization*, DOE/RL-96-0004, Rev. 1, U.S. Department of Energy, Richland Washington, June 2, 1998.

DOE-RL, 1998b, *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors*, DOE/RL-96-0006, Rev. 1, U.S. Department of Energy, Richland Washington, July 1998.

Marshall F. et al., 1998, "Common-Cause Failure Parameter Estimations," NUREG/CR-5497, Idaho National Engineering and Environmental Laboratory & University of Maryland for the U.S. Nuclear Regulatory Commission, October 1998.

Sellafield, 1998, "Sellafield Reliability Database," Version 3.0, British Nuclear Fuels Plc, Last Modified 7/7/98 (Proprietary Information).

Swain A. and Guttmann H., 1983, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," [Technique for Human Error Prediction (THERP)]," NUREG/CR-1278, Sandia National Laboratories for the US Nuclear Regulatory Commission, August 1983.